CLAIMS

Claims 1 through 10 (Cancelled).

11. (New) A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature certify contents that are to be included in the public key certificate, out of contents registered with the registration authority;

generating, by the registration authority, a certificate issuing request including the contents signed by the registration authority and the registration authority signature;

sending the certificate issuing request from the registration authority to the issuing authority; and

generating, by the issuing authority, the public key certificate including the contents signed by the registration authority, the registration authority signature, issuing contents issued by the issuing authority, and an issuing authority signature signed by the issuing authority to certify the contents signed by the registration authority, the registration authority signature and issuing contents issued by the issuing authority.

12. (New) A method as recited in claim 11, wherein

the contents signed by the registration authority is a predetermined identifier to specify information to be certified by the pubic key certificate of the end entity.

13. (New) A method as recited in claim 11, wherein

the contents signed by the registration authority is a hash value calculated by applying a hash function to information to be certified by the public key certificate of the end entity.

14. (New) A method for as recited in claim 11, further comprising the steps of:

verifying, by a verifying party, the issuing authority signature with the contents signed by the issuing authority; and

verifying, by the verifying party, the registration authority signature with the contents signed by the registration authority included in the public key certificate.

15. (New) A method as recited in claim 12, further comprising the steps of:

acquiring, by a verifying party, information signed by the registration authority according to the identifier in the public key certificate;

calculating, by the verifying party, a hash value of the acquired information;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

16. (New) A method as recited in claim 13, further comprising the steps of:

calculating, by a verifying party, a hash value of the information signed by the registration authority in the public key certificate;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

17. (New) A method as recited in claim 14, further comprising the steps of:

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party, up to the public key certificate;

verifying, by the verifying party, the registration authority signature described in the public key certificate using the public key of the registration authority; and

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party up to the public key certificate of the registration authority.

18. (New) A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority from a public key certificate database of the issuing authority according to the registration authority name described on the public key certificate.

19. (New) A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority described in an extended region of the public key certificate to be verified.

20. (New) As method as recited in claim 11, further comprising the steps of:

sending, by the registration authority, a certificate invalidation request to the issuing authority of the public key certificate of the registration authority;

receiving, by the issuing authority, the certificate invalidation request; and

invalidating, by the issuing authority, the public key certificate of the registration authority.